

# **NATIONAL POLAR-ORBITING OPERATIONAL ENVIRONMENTAL SATELLITE SYSTEM (NPOESS)**

## **SECURITY CLASSIFICATION GUIDE**

### **PART I OF II**

30 October 1996



NPOESS IPO  
8455 Colesville Rd, Ste 1450  
Silver Spring MD 20910

Distribution is limited to  
United States Government agencies and their contractors  
For official and administrative use  
Other agencies requests for this document shall be referred to the NPOESS IPO

“Destruction notice - For classified documents, follow the procedures of DoD 5220.22-M, Industrial Security Manual, Section 11-19, or DoD 5200.1-R, Information Security Program Regulation, Chapter

X. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.”

National Polar-orbiting Operational Environmental Satellite System  
Integrated Program Office  
8455 Colesville Rd, Ste 1450  
Silver Spring MD 20910

## FOREWORD

1. **System Description:** A complete description of NPOESS is contained in the Program Protection Plan (PPP). In general, the system is designed to integrate and update the space-based remote sensing capability of the military and the civil government agencies. The primary basis for the enhanced capability is the Defense Meteorological Satellite Program (DMSP) and a series of National Oceanic and Atmospheric Administration (NOAA) satellites which serve the non-military community.

NPOESS is designed to provide for the acquisition of global and regional cloud cover imagery and specialized meteorological, climatic, terrestrial, oceanographic, solar-geophysical, and other data for a period of at least ten years. The program also provides for the transmission of this data to ground stations, data processing and dissemination of data to all users worldwide. It will support existing Department of Commerce (DOC) and National Aeronautics and Space Administration (NASA) mission requirements as well as Department of Defense (DoD) peacetime and wartime missions.

NPOESS system will consist of the following four segments: a) a Space (on-orbit) Segment, b) a Launch Support Segment, c) a Command, Control and Communications (C<sup>3</sup>) Segment, and d) an Interface Data Processor (IDP) Segment.

The concept of operations for NPOESS includes data collection by satellites flying in sun-synchronous, near polar orbits. Each satellite will carry a variety of sensors to provide both military and civil environmental data. Pending an international agreement, payloads will be exchanged between the US Government (USG) and European Space Agency/European Meteorological Satellite Program (ESA/EUMETSAT) in Europe.

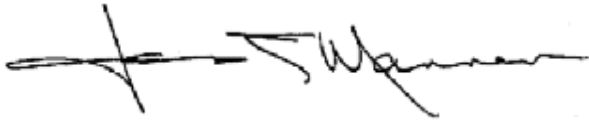
A primary goal of NPOESS is a standardized approach to permit compatibility, interoperability, interchangeability, and commonality among DoD, DOC, and NASA systems, components and interfaces.

2. **Authority:** This guide is issued under authority of DoD 5200.1-R & AFI 31-401, Information Security Regulation/Instruction.

**3. Reference Documents:**

- a. Executive Order 12958, Classified National Security Information, dated 17 April 1995
- b. Implementation Management Plan, Amendment to DoD Space Policy, AFSPC/SP, dated 20 April 1994
- c. AFSPC/SP Memorandum, Modernization Planning Process Protection Guidelines, dated 15 May 1995
- d. NPOESS Program Protection Plan

Approved by:

A handwritten signature in black ink, appearing to read 'J. T. Mannen', written over a horizontal line.

---

JAMES T. MANNEN, SES  
System Program Director  
National Polar-Orbiting Operational Environmental Satellite System

## **SUMMARY OF CHANGES**

1. This is the first issue of NPOESS Security Classification Guide.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
Summary of Changes.....	3
Table of Contents.....	4
General Instructions.....	5
Release of Information.....	8
Classification Guidance .....	10
List of Acronyms .....	15
Distribution List.....	16
Sample SCG Letter Change Format .....	21

## SECTION I

### GENERAL INSTRUCTIONS

1. Purpose: This guide identifies specific information developed during various phases of NPOESS requiring protection in the interest of national security. The primary objective is the protection of information related to designs; technologies; data collection, processing and dissemination techniques; operations; and special missions inherent in the system. This document has been approved by an original classification authority and is consistent with national security classification guidance set forth in executive order and implementing directives of the USG.

2. Office of Primary Responsibility (OPR): This guide is issued by:

National Polar-orbiting Operational Environmental Satellite System  
Integrated Program Office  
8455 Colesville Rd, Ste 1450  
Silver Spring MD 20910  
(301) 427-2070

3. Classification Recommendations:

a. If the security classifications in this guide impose impractical policies, procedures, or requirements; if current conditions, changes, or progress attained in this effort, scientific, or technological changes in the state-of-the-art, or any other contributory factors indicate a need for changes, forward your recommendations to the NPOESS IPO. Users are encouraged to help improve and maintain the currency of this guide. Pending final decision, handle and protect the items of information involved at the highest present or recommended classification. Users of this guide are encouraged to assist in improving and maintaining the currency and adequacy of this guide.

b. In the event of conflict between this guide and security classification guidance of related programs, address the issue to the NPOESS IPO for resolution. Until a conflict is resolved, the information involved shall be protected at the highest level required by any of the "conflicting" classification guides.

## SECTION I (Cont'd)

4. Application, Reproduction, and Dissemination: Specified groups involved in NPOESS, including industrial activities, may make reproductions and extracts of portions of this guide.
5. Classification Currency: Changes to this guide are made by letter, (e.g., Subject: Letter Change No. \_\_\_, NPOESS IPO, Security Classification Guide, (30 Oct 96)). These letters indicate the appropriate change and authority for such change. If the change (or revision) changes a declassification instruction on existing classified documents or material from a specific date or event to Exemptions and Extensions in accordance with Executive Order 12958 "Classified National Security Information", notify all holders of the information. Follow the requirements of DoD 5200.1-R/AFI 31-401. The following is a sample statement that may be included: "Remark all information classified under the previous (or basic) classification guide and mark for declassification on 30 October 2006 according to this guide (or changes)." The authority is this guide and the effective date is the date of the guide. Upon receipt of a letter change, make the appropriate change and file the letter of authority in the back of the guide.
6. "For Official Use Only" (FOUO): For Official Use Only (FOUO) is not a security classification. Handle, protect, and dispose of FOUO information according to AFI 37-131. For contractors, handle, protect and dispose of FOUO information in accordance with DD Form 254.
7. Manufacture, Test, and Assemble: During manufacture, test, and assembly processes, the classification assigned by this guide applies at the earliest point when classified information concerning design, performance, and/or other classified characteristics can be derived from or traced to NPOESS.
8. Disassembly and Repair: During disassembly and repair, the classification assigned by this guide no longer applies at the earliest point where classified information concerning design, performance, or other classified characteristics can no longer be derived from or traced to NPOESS.
9. Disassociation, Masking, and Coding: Only the originating activity may authorize or direct these procedures.
10. TEMPEST: Consider TEMPEST requirements as discussed in the NPOESS Program Protection Plan for all appropriate facilities and equipment associated with the program. Specific guidance on TEMPEST measures and requirements is contained in AFI 33-201.
11. Previously Unclassified Data: Data used and applied in the program which was previously unclassified shall remain unclassified unless it specifically reveals information designated as classified in this guide when associated with NPOESS. Such data will then be handled according to the National Industrial Security Program Operating Manual (NISPOM) for contractors or DoD 5200.1-R/AFI 37-401. All data created after the date of this guide will be properly classified by this guide and will be properly marked and controlled.

12. Operations Security (OPSEC):

a. OPSEC is the systematic and analytical process by which the USG and its supporting contractors deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities and operations. Information generally available to the public as well as certain detectable activities may reveal the existence of, and sometimes details about, classified or sensitive information or undertakings.

b. USG organizations must establish and maintain OPSEC programs in accordance with the DoC Information Security Manual (OCT 94) . Contractors will comply with OPSEC program requirements as specified in contracts. OPSEC efforts may either support the conduct of USG/contractor operations and activities, or the development and integration of OPSEC measures into systems through systems security engineering, or both.

c. This guide does not establish OPSEC program policies, procedures, or requirements. It does identify the security classification of specific OPSEC related information which may develop regarding programs.

13. Technology Transfer: A major goal of USG classification strategy is to deny potential adversaries access to information, hardware and technology that will enable them to accelerate their military programs and simultaneously reduce the effectiveness of US national or military capabilities. Foreign dependence on the US for certain advanced technologies is described in the NPOESS Program Protection Plan. This information should be considered when formulating any classification guidance or establishing any other security requirements. Specific guidance for protecting NPOESS-related technologies is contained in the Program Protection Plan and the Technology Control Plan for this program.



## SECTION II

### RELEASE OF INFORMATION

#### 1. Public Release.

a. The fact that this guide shows certain details of information as unclassified does not permit automatic public release of the information. Send proposed public disclosures of unclassified information regarding NPOESS to the NPOESS IPO, Public Affairs for such approval. Follow local guidance for suspenses and lead time, however, the following typically applies:

- For domestic release - submit three copies, 30 days prior to proposed publication or presentation.
- For International release - submit seven copies, 45 days prior to proposed publication or presentation. (Additional copies and time is required for coordination with the appropriate Foreign Disclosure Policy Office.)

b. The term "information" applies, but is not limited to, articles, speeches, photographs, brochures, advertisements, displays, and presentations on any phase of NPOESS.

c. Defense contractors and other agencies must screen all information they submit for determination of releasability to insure it is unclassified and technically accurate. The letter of transmittal must certify this review. Copies of the material may not be released outside official channels until the review process is complete. If you find information during the review process that you suspect is classified, notify all holders of the level of classification required. When doubt exists concerning the classified status of a proposed release pertaining to this program, the NPOESS IPO makes the final decision. The material submitted for review must include a valid suspense date, if applicable.

d. Only information that has been reviewed and certified for public release may be released. Submit information developed after initial approval for public release for review and further processing as outlined in a and b above.

e. Material which requires an export license may not be entered into security review channels for public release approval to circumvent the licensing requirements of the Departments of State and Commerce.

f. Obtain approval for planned or contemplated visits of public media representatives from the NPOESS IPO.

2. Release of Classified Information to Foreign Governments or their representatives. Any military activity or defense contractor receiving a request from a foreign government or representative thereof for classified information pertaining to NPOESS must send the request to the NPOESS IPO. Military activities must process such requests as outlined in AFI 16-201. Contractors who wish to honor such requests rather than send them to the Foreign Disclosure Office, must apply for an export license according to the International Traffic in Arms Regulation (ITAR) and notify the military of their intent to apply for such license.

3. Release of Unclassified Technical Information (Not Approved for Public Release) to US Citizens or Foreign Nationals Residing in a foreign Country: Such requests must be reported to the program OPR for a releasability determination. Contractors or non-government agencies possessing NPOESS information may apply for an export license through the Department of State, but must notify the program OPR of such an application and must meet all requirements of the Department of State and Department of Commerce for export of technical data pertaining to military systems.

4. Approved Release of Information for Foreign Governments. Some program information may be releasable to foreign governments and agencies participating in NPOESS under an approved Delegation of Disclosure Letter or similar sanctioned agreement. Questions should be referred to the servicing Foreign Disclosure Policy Office and the program OPR.

## SECTION III

### CLASSIFICATION GUIDANCE

Under Executive Order 12958, Sections 1 and 2, this guide identifies the concise reasons for the classification of information. It also identifies the category of specific information that is deemed to be exempt from declassification within 10 years. The classification table that follows includes a “reason” column that lists one of seven numbered categories identifying why the information is being classified. It also includes an “exemption” column for information which is exempt from the required 10 year classification limit. Following are keys to the number codes used in those columns.

#### REASON (Classification Categories)

1. Military plans, weapons systems or operations.
2. Foreign Government Information.
3. Intelligence Activities (including special activities), intelligence sources or methods, or cryptology.
4. Foreign relations or foreign activities of the United States, including confidential sources.
5. Scientific, technological or economic matters relating to the national security.
6. USG programs for safeguarding nuclear materials or facilities.
7. Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security.

#### EXEMPTION (Exemption Categories)

At the time of original classification, information may be exempted from the 10 year declassification requirement when that specific information could reasonably be expected to cause damage to the national security for a greater period, and its release could reasonably be expected to:

1. Reveal an intelligence source, method or activity, or a cryptologic system or activity;
2. Reveal information that would assist in the development or use of weapons of mass destruction;
3. Reveal information that would impair the development or use of technology within a United States weapons system;
4. Reveal United States military plans or national security emergency preparedness plans;
5. Reveal foreign government information;
6. Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a greater period; or
7. Violate a statute, treaty or international agreement.

### NPOESS Security Classification Guidance

INFORMATION REVEALING:	CLASSIF DECLASS:	REASON	EXEMP- TION	REMARKS
<b>1.0 System Description</b>				
1.1 The NPOESS mission, purpose and goals	U			
1.2 The joint effort between DoD and the National Oceanic and Atmospheric Administration (NOAA)	U			
1.3 Participation of, and cooperation with foreign partners	U			
1.4 Specific impacts to missions supported due to the loss of NPOESS data or capability.	S 30 Oct 06	1, 3		
1.5 Special and/or wartime/contingency mission aspects and related command and control procedures.	S EXEMPT	1, 3	4	
<b>2.0 Space Segment</b>				
<b>2.1.0 Spacecraft Systems</b>				
2.1.1 Overall spacecraft design and configuration.	See Remarks			Classification depends on specific aspect of design. Consider for earlier declass if appropriate.
2.1.1.1 Generic information.	U			
2.1.1.2 Technical details revealing unique propulsion, attitude control, dimensional stability or structural technologies employed.	S 30 Oct 06	5		
<b>2.2.0 Sensors and Payload</b>				
2.2.1 Details of specific sensor and payload integration approach for the spacecraft.	S 30 Oct 06	5		Consider for earlier declass if technology changes dictate.

INFORMATION REVEALING:	CLASSIF DECLASS:	REASON	EXEMP- TION	REMARKS
2.2.2 Special Purpose sensors and sensor packages.	S 30 Oct 06	5, 3		Classification depends on specific aspect of sensor environmental requirements.
2.2.3 Special sensor environmental requirements (including cooling, power, etc.).	See Remarks			
2.2.3.1 When related to mature technology and common sensors.	U			
2.2.3.2 When related to sensors listed in item 2.2 above or revealing potential weaknesses which could be subject to exploitation.	S 30 Oct 06	5		
2.2.4 Vulnerability of sensors to environmental and external effects (including radiation, heat, ECM, optical countermeasures, etc.).	S EXEMPT	7	3, 4	
2.2.5 Protective measures or capabilities against such effects.	S EXEMPT	7, 1	3, 4	Locations are in general unclassified, however deploying agencies may choose to classify certain deployments.
<b>3.0 Command and Control Segment</b>				
3.1 Geographic locations of stations				
<b>4.0 IDPS Segment</b>				Consider for earlier declass if technology changes dictate.
4.1 Details of high resolution downlink techniques and data protection measures.	S 30 Oct 06	5, 1		
4.2 Unique signal processing techniques associated with data processing.	S 30 Oct 06	5		
<b>5.0 Launch Segment</b>				Classification depends on aspect of launch ops and specific nature of mission.
5.1 Specific launch support details associated with special and/or wartime/contingency missions.	See Remarks			

INFORMATION REVEALING:	CLASSIF DECLASS:	REASON	EXEMP- TION	REMARKS
5.1.1 Facts normally releasable in connection with sensitive military space launch operations.	U			
5.1.2 Details which could compromise mission integrity or identify the specific nature of the launch or the classified national security operation it supports.	S EXEMPT	1	4	
<b>6.0 Vulnerability and Survivability</b>				
6.1 Vulnerability of data processing functions (IDP Segment) to all forms of intentional degradation including physical damage, ECM, computer intrusion, intelligence penetration, data denial, data alteration, network damage, etc..	S EXEMPT	7	3, 4	
6.2 Vulnerability of on-orbit control function (C3 segment) to the same .	S 30 Oct 06	7		
6.3 Details of system performance and operational effectiveness under various routine and threat/hostile/stressed conditions.	S EXEMPT	5, 1, 7	3, 4	
<b>7.0 System Security</b>				
7.1 COMSEC equipment and techniques employed to protect telemetry, satellite control functions and operational data.	See Remarks			Comply with classification guidance for cryptographic material and equipment. See AFSM 4200, dated 25 Jun 93.
7.2 Protection techniques including radiation hardening, ECCM and optical counter-countermeasures.	S EXEMPT	5, 7	3, 4	
<b>8.0 Emerging Technology</b>				
8.1 Specific MMIC technology integration into system sensors.	S 30 Oct 06	5		Consider for earlier declass if technology changes dictate.
8.2 Focal Plane Array layout and thermal control techniques.	S 30 Oct 06	5		Consider for earlier declass if technology changes dictate.

INFORMATION REVEALING:	CLASSIF DECLASS:	REASON	EXEMP- TION	REMARKS
8.3 Details of specialized antenna design and construction.	See Remarks			Classification depends on aspect of antenna design or manufacture. Consider for earlier declass if technology changes dictate.
8.3.1 Generic antenna design features common to non-sensitive space platforms and systems.	U			
8.3.2 Details of specialized manufacturing techniques or unique design features not common to non-sensitive space platforms.	S 30 Oct 06	5		
8.4 Advanced computing and opto-electronic technologies employed in data fusion, processing and distribution operations.	S 30 Oct 06	5		Consider for earlier declass if technology changes dictate.
<b>9.0 Operations</b>				

## **SECTION IV**

### **LIST OF ACRONYMS**

<b>AFI</b>	<b>Air Force Instruction</b>
<b>AFMC</b>	<b>Air Force Materiel Command</b>
<b>AFSPC</b>	<b>Air Force Space Command</b>
<b>C3</b>	<b>Command, Control and Communications</b>
<b>COMSEC</b>	<b>Communications Security</b>
<b>DOC</b>	<b>Department of Commerce</b>
<b>DoD</b>	<b>Department of Defense</b>
<b>ECCM</b>	<b>Electronic Counter-Countermeasures</b>
<b>ECM</b>	<b>Electronic Countermeasures</b>
<b>EPITS</b>	<b>Essential Program Information, Technology and Systems</b>
<b>ESA</b>	<b>European Space Agency</b>
<b>EUMETSAT</b>	<b>European Meteorological Satellite</b>
<b>FOUO</b>	<b>For Official Use Only</b>
<b>IDP</b>	<b>Interface Data Processor</b>
<b>ITAR</b>	<b>International Traffic in Arms Regulation</b>
<b>MMIC</b>	<b>Monolithic Microwave Integrated Circuits</b>
<b>NASA</b>	<b>National Aeronautics and Space Administration</b>
<b>NOAA</b>	<b>National Oceanic and Atmospheric Administration</b>
<b>NPOESS</b>	<b>National Polar-Orbiting Operational Environmental Satellite System</b>
<b>OPR</b>	<b>Office of Primary Responsibility</b>
<b>SMC</b>	<b>Space and Missile Center (USAF)</b>



**SECTION V**  
**DISTRIBUTION LIST**

<u>Activity</u>	<u>Number of copies</u>
Director of Information Security Review OASD/PA Room 2C757 (Public Affairs) 1400 Pentagon Washington. DC 20301-1400	1
Deputy Undersecretary of Defense for Policy OASD (C31) OD ASD (CI/SCM) ISS Room 3C274 The Pentagon Washington. DC 20310-3040	1
Defense Technical Information Center ATTN.: DTIC-ZM 5010 Duke Street Bldg. 5 Cameron Station Alexandria, VA 22304-6145	1
SAF/PAS/SN/SX/AQS/XO 1690 Air Force Pentagon Washington. DC 20330-1690	1 ea
HQ AFSPA/SPIB 8201 H Avenue SE Kirtland AFB, NM 87117-6001 Attn.: Security Manager	1
HQ AFSPC/DO/DR/SP 150 Vandenberg Street Suite 1105 Peterson AFB CO 80914-4200	1 ea
HQ AFMC/SPX/PA 4225 Logistics Ave Suite 21 Wright Patterson AFB, OH 45433-5001	1 ea
HQ SMC/SDAP/IND/CL/CI 2420 Vela Way Suite 1467 Los Angeles AFB, CA 90245-4659	1 ea

National Polar-orbiting  
Operational Environmental Satellite System  
SECURITY CLASSIFICATION GUIDE

30 OCT 96

Aerospace Corporation 2350 East El Segundo Blvd. El Segundo, CA 90245-4691 Attn.: Classification Office M2-100	1
Director NSA 9800 Savage Road Ft. George G. Mead, MD 20755-6006	1
Director of Security HQ DIS Industrial Security Office (V0410) 1900 Half St. Washington. DC 20324	1
DIS, Director of Industrial Security Capital Region 2461 Eisenhower Ave. Alexandria, VA 22331-1000	1
DIS, Director of Industrial Security Mid-Atlantic Region 1040 Kings Highway North Cherry Hill, NJ 08034-1908	1

DIS, Director of Industrial Security Mid-Western Region Federal Office Bldg. 610 Canal Street, room 800 Chicago, IL 60607-4599	1
DIS, Director of Industrial Security New England Region Barnes Bldg. 495 Summer Street Boston, MA 02210-2192	1
DIS, Director of Industrial Security North-Western Region Presidio of San Francisco San Francisco, CA 94129-7700	1
DIS, Director of Industrial Security Pacific Region 3605 Long Beach Blvd., Suite 405 Long Beach, CA 90807-4013	1
DIS, Director of Industrial Security South-Eastern Region 2300 Lake Park Drive, Suite 250 Smyrna, GA 30080-7606	1
DIS, Director of Industrial Security South-Western Region 106 Decker Court Irving, TX. 75062-2795	1
AFPEO/SP 1110 Air Force Pentagon Room 4D279 Washington, DC 20330-1110	1
HQ AFOTEC/SP 8500 Gibson Boulevard S.E. Kirtland AFB NM 87117-5558	1 ea

HQ USAF/SPI 1340 Air Force Pentagon Washington DC 20330-1340	1
SAF/AAZD c/o HQ AU 55 LeMay Plaza South Maxwell AFB AL 36112-1690	1
HQ AFHSO/HOS 170 Luke Avenue Suite 400 Bolling AFB DC 20332-5113	1
HQ AFHA/ISR 600 Chennault Circle Maxwell AFB AL 36112-6424	1
Chief of Naval Operations (N6) 2000 Navy Pentagon Washington DC 20350-2000	1
Chief of Naval Operations (N096) U S Naval Observatory 34th and Massachusetts Ave NW Washington DC 20392-5100	1
Commander, Space and Naval Warfare Systems Command (PMW 175) 2451 Crystal Drive Arlington, VA 22245-5200	1
Commander, Naval, Meteorology and Oceanography Command 1020 Balch Blvd Stennis Space Center, MS 39529-5005	1
Commandant of the Marine Corps HQ US Marine Corps Attn: ASL-44 Washington DC 20380	1

National Polar-orbiting  
Operational Environmental Satellite System  
**SECURITY CLASSIFICATION GUIDE**

30 OCT 96

NOAA Security Officer 1  
Attn: Alan Brown  
1315 East West Highway  
Room 3609  
Silver Spring, MD 20910

NASA/GSFC 1  
Code 205.1/Security Branch  
Greenbelt MD 20771

**APPENDIX**

**SAMPLE SCG LETTER CHANGE FORMAT**

MEMORANDUM FOR ALL RECIPIENTS OF SUBJECT GUIDE    DATE

FROM; ( Appropriate Program Office)

Letter Change #\_\_ to the (Appropriate SCG Title and Date)

1. Request the following (PEN AND INK CHANGES/PAGE SUBSTITUTIONS) be made to the subject guide:

a. Page \_\_. Section \_\_. item \_\_: (PROVIDE APPROPRIATE GUIDANCE)

2. (IF APPROPRIATE, PROVIDE REASONS FOR CHANGES)

3. Upon completion of the above change, place this letter in the back of the guide as authority for these changes.

SIGNATURE